

What is claimed is:

- 1 1. A production protection system dealing with  
2 contents that are digital production, comprising:  
3 obtaining means for obtaining data including at  
4 least one of a first content, on which first encryption  
5 has been performed and a second content, on which second  
6 encryption has been performed, the second encryption is  
7 more difficult to break than the first encryption;  
8 first content decryption means for decrypting the  
9 first content using a first decryption method that  
10 corresponds to the first encryption when the data that has  
11 been obtained by the obtaining means includes the first  
12 content; and  
13 second content decryption means for decrypting the  
14 second content using a second decryption method that  
15 corresponds to the second encryption and is more difficult  
16 than the first decryption method when the data that has  
17 been obtained by the obtaining means includes the second  
18 content.
- 1 2. The production protection system according to  
2 Claim 1, wherein  
3 the obtaining means and the first content  
4 decryption means are realized by a personal computer that  
5 executes software for decrypting contents, and

6 the second content decryption means is realized by  
7 one of tamperproof hardware and an apparatus that executes  
8 tamperproof software.

1 3. The production protection system according to  
2 Claim 2, wherein the obtaining means obtains the data by  
3 receiving the data from an outside network,

4 the production protection system, further  
5 comprising:

6 replay means for audio-visually replaying the  
7 first content that has been decrypted by the first content  
8 decryption means;

9 encryption means for performing third encryption,  
10 which is different from the second encryption, on the  
11 second content that has been decrypted by the second  
12 content decryption means; and

13 recording means for recording at least part of the  
14 second content on which the third encryption has been  
15 performed by the encryption means on a recording medium.

1 4. The production protection system according to  
2 Claim 3, wherein the encryption means and a data  
3 communication channel between the second content  
4 decryption means and the encryption means are realized by  
5 one of tamperproof hardware and an apparatus that executes  
6 tamperproof software.

1 5. The production protection system according to  
2 Claim 3, wherein an encryption algorithm that is used by  
3 the second content decryption means partially differs from  
4 an encryption algorithm that is used for encryption by the  
5 encryption means.

1 6. The production protection system according to  
2 Claim 3, further comprising:

3 PC connecting means for connecting to the personal  
4 computer via a predetermined interface; and

5 recording medium loading means where the recording  
6 medium is set, wherein

7 the second content decryption means, the  
8 encryption means, the recording means, the PC connecting  
9 means, and the recording medium loading means are realized  
10 by a piece of hardware,

11 the second content decryption means obtains the  
12 second content in the data that has been obtained by the  
13 obtaining means via the PC connecting means and decrypts  
14 the obtained second content, and

15 the recording means records the second content on  
16 the recording medium that has been set in the recording  
17 medium loading means.

1 7. The production protection system according to  
2 Claim 2, wherein

3           the data that is to be obtained by the obtaining  
4 means includes control information, which has been  
5 encrypted, for controlling operations on each content  
6 included in the obtained data, and  
7           at least one of the first content decryption means  
8 and the second content decryption means includes a control  
9 information decryption unit for decrypting the control  
10 information.

1 8.       The production protection system according to  
2 Claim 7, wherein  
3           the second content decryption means includes the  
4 control information decryption unit, and  
5           the personal computer that realizes the second  
6 content decryption means further executes software for  
7 decrypting the control information.

1 9.       The production protection system according to  
2 Claim 8, wherein  
3           the control information includes a key used for  
4 decrypting the second content,  
5           the control information decryption unit further  
6 includes a first authentication encryption unit, and  
7           the second content decryption means further  
8 includes a second authentication encryption unit,  
9 wherein

10           the first authentication encryption unit  
11 performs authentication of the second authentication  
12 encryption unit, performs encryption communication with  
13 the second authentication encryption unit, and transmits  
14 the key in the control information that has been decrypted  
15 by the control information decryption unit to the second  
16 authentication encryption unit when the authentication  
17 is successfully performed,

18           the second authentication encryption unit  
19 performs authentication of the first authentication  
20 encryption unit, performs encryption communication with  
21 the first authentication encryption unit, and obtains  
22 the key, and

23           the second content decryption means decrypts the  
24 second content using the key that the second  
25 authentication encryption unit has obtained.

1 10.       The production protection system according to  
2 Claim 1, wherein

3           the obtaining means and the first content  
4 decryption means are realized by an apparatus that  
5 executes software for decrypting contents, and

6           the second content decryption means is realized by  
7 one of tamperproof hardware and an apparatus that executes  
8 tamperproof software.

1 11. The production protection system according to  
2 Claim 10, wherein  
3 the obtaining means obtains the data by receiving  
4 the data from an outside network, and  
5 the first content and the second content are same  
6 production that is expressed by digital data in different  
7 styles.

1 12. The production protection system according to  
2 Claim 11, further comprising:  
3 encryption means for performing third encryption,  
4 which is different from the second encryption, on the  
5 second content that has been decrypted by the second  
6 content decryption means; and  
7 recording means for recording at least part of the  
8 second content on which the third encryption has been  
9 performed by the encryption means on a recording medium.

1 13. The production protection system according to  
2 Claim 12, wherein the encryption means and a data  
3 communication channel between the second content  
4 decryption means and the encryption means are realized by  
5 one of tamperproof hardware and an apparatus that executes  
6 tamperproof software.

1 14. The production protection system according to

2 Claim 12, wherein

3 the first content is a music content for trial,

4 and

5 the second content is a music content for sale and

6 has a higher audio quality than the first content.

1 15. The production protection system according to

2 Claim 14, further comprising replay means for replaying

3 the first content that has been decrypted by the first

4 content decryption means.

1 16. The production protection system according to

2 Claim 12, wherein an encryption algorithm that is used by

3 the second content decryption means partially differs from

4 an encryption algorithm that is used for encryption by the

5 encryption means.

1 17. The production protection system according to

2 Claim 12, wherein

3 the encryption means includes:

4 a master key storage unit for storing a master key

5 in advance;

6 a disk key creation unit for creating a disk key;

7 a disk key encryption unit for encrypting the disk

8 key that has been created by the disk key creation unit

9 using the master key;

10           a title key creation unit for creating a title  
11 key;  
12           a title key encryption unit for encrypting the  
13 title key that has been created by the title key creation  
14 unit using the disk key; and  
15           a content encryption unit for encrypting at least  
16 part of the second content that has been decrypted by the  
17 second content decryption means using the title key, and  
18           the recording means records the disk key that has  
19 been encrypted by the disk key encryption unit, the title  
20 key that has been encrypted by the title key encryption  
21 unit, and the second content that has been encrypted by  
22 the content encryption unit on the recording medium.

1 18.       The production protection system according to  
2 Claim 17, wherein  
3           inherent information that is inherent in the  
4 recording medium is recorded on the recording medium in  
5 advance, and  
6           the disk key creation unit creates the disk key  
7 according to the inherent information on the recording  
8 medium.

1 19.       The production protection system according to  
2 Claim 17, wherein the title key creation unit creates the  
3 title key according to information, which is part of the



4 second content that has been decrypted by the second  
5 content decryption means.

1 20. The production protection system according to  
2 Claim 12, wherein

3 an inherent disk key inherent in the recording  
4 medium that has been encrypted using a master key is  
5 recorded on the recording medium in advance,

6 the encryption means includes:

7 a master key storage unit for storing the master  
8 key in advance;

9 a disk key creation unit for creating a disk key  
10 by decrypting the inherent disk key on the recording  
11 medium using the master key;

12 a title key creation unit for creating a title  
13 key;

14 a title key encryption unit for encrypting the  
15 title key that has been created by the title key creation  
16 unit using the disk key; and

17 a content encryption unit for encrypting at least  
18 part of the second content that has been decrypted by the  
19 second content decryption means using the title key, and

20 the recording means records the title key that has  
21 been encrypted by the title key encryption unit and the  
22 second content that has been encrypted by the content  
23 encryption unit on the recording medium.

1 21. The production protection system according to  
2 Claim 12, wherein  
3 the recording medium includes a recording  
4 apparatus authentication unit for transmitting  
5 authentication information, and  
6 the recording means judges correctness of the  
7 recording medium according to the authentication  
8 information that has been transmitted from the recording  
9 apparatus authentication unit, and performs the  
10 recording, in which at least part of the second content on  
11 which the third encryption has been performed is recorded  
12 on a recording medium, only when the recording medium is  
13 correct.

1 22. The production protection system according to  
2 Claim 10, further comprising:  
3 encryption means for performing third encryption,  
4 which is different from the second encryption, on the  
5 second content that has been decrypted by the second  
6 content decryption means; and  
7 recording means for recording at least part of the  
8 second content on which the third encryption has been  
9 performed by the encryption means on a recording medium.

1 23. The production protection system according to  
2 Claim 22, wherein an encryption algorithm that is used by

3 the second content decryption means partially differs from  
4 an encryption algorithm that is used for encryption by the  
5 encryption means.

1 24. The production protection system according to  
2 Claim 10, wherein

3 the data that is to be obtained by the obtaining  
4 means includes first content charging information, which  
5 is charging information on decryption of the first content  
6 when the data to be obtained includes the first content,  
7 and the data that is to be obtained includes second  
8 content charging information, which is charging  
9 information on decryption of the second content when the  
10 data to be obtained includes the second content,

11 the first content decryption means performs a  
12 charging operation according to the first content charging  
13 information when the first content is decrypted, and

14 the second content decryption means performs the  
15 charging operation according to the second content  
16 charging information when the second content is decrypted.

1 25. The production protection system according to  
2 Claim 1, wherein

3 the first encryption is performed using a first  
4 key,

5 the second encryption is performed using a second

6 key, which has a larger data size than the first key,  
7 the data that is to be obtained by the obtaining  
8 means further includes control information, which has the  
9 first and second keys, for controlling operations on each  
10 content included in the data to be obtained,  
11 the first content decryption means decrypts the  
12 first content using the first key, and  
13 the second content decryption means decrypts the  
14 second content using the second key.

1 26. The production protection system according to  
2 Claim 25, wherein  
3 the control information is encrypted using a  
4 control key that has been derived from a third key and a  
5 system common key, and included in the data that is to be  
6 obtained by the obtaining means,  
7 the third key is encrypted using a fourth key and  
8 included in the data that is to be obtained,  
9 the first content decryption means includes a  
10 first control information decryption unit for storing the  
11 system common key and a fifth key corresponding to the  
12 fourth key in advance, decrypting the third key using the  
13 fifth key, deriving the control key from the decrypted  
14 third key and the system common key, and decrypting the  
15 control information using the control key, and  
16 the second content decryption means includes a

17 second control information decryption unit for storing the  
18 system common key and the fifth key corresponding to the  
19 fourth key in advance, decrypting the third key using the  
20 fifth key, deriving the control key from the decrypted  
21 third key and the system common key, and decrypting the  
22 control information using the control key.

1 27. A production protection system that deals with  
2 music contents for trial, on which first encryption has  
3 been performed, and music contents for sale, on which  
4 second encryption has been performed, a music content for  
5 sale is same music as a music content for trial and has a  
6 higher audio quality than the music content for trial,  
7 the production protection system, comprising:  
8 obtaining means for obtaining data that is a  
9 combination of a music content for trial and a music  
10 content for sale from an outside network;  
11 first content decryption means for decrypting a  
12 first content in the data that has been obtained by the  
13 obtaining means using a first decryption method;  
14 replay means for replaying a music of the first  
15 content that has been decrypted by the first content  
16 decryption means;  
17 second content decryption means for decrypting a  
18 second content in the data that has been obtained by the  
19 obtaining means using a second decryption method, which is

20 more complicated than the first decryption method;  
21 encryption means for performing third encryption,  
22 which is different from the second encryption, on the  
23 second content that has been decrypted by the second  
24 content decryption means; and  
25 recording means for recording at least part of the  
26 second content on which the third encryption has been  
27 performed by the encryption means on a recording medium,  
28 wherein  
29 the obtaining means and the first content  
30 decryption means are realized by a personal computer that  
31 executes software for decrypting contents, and  
32 the second content decryption means, the  
33 encryption means, and a data communication channel between  
34 the second content decryption means and the encryption  
35 means are realized by one of tamperproof hardware and an  
36 apparatus that executes tamperproof software.

1 28. The production protection system according to  
2 Claim 27, wherein an encryption algorithm that is used by  
3 the second content decryption means partially differs from  
4 an encryption algorithm that is used for encryption by the  
5 encryption means.